学校编码：10384　　分类号_____ 密级_____

学号：19020101152513　　UDC_____

硕 士 学 位 论 文

实现任意布尔函数访问结构的特征加密方案

Attribute-Based Encryption with Arbitrary Boolean Function Access Control

李 明

指导教师姓名：曾 吉 文 教授

专 业 名 称：基 础 数 学

论文提交日期：2013 年 6 月

论文答辩日期：2013 年 6 月

学位授予日期：

答辩委员会主席：_____

评 阅 人：_____

2013 年 6 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1、保密　（　），在　　年解密后适用本授权书。

2、不保密（　）

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

中文摘要

特征加密方案（ABE）通过在密文和密钥之间规定访问规则，有效地解决了匿名访问控制问题。在密文规则的特征加密方案（CP-ABE）中，每个用户与一个特征集相对应，数据通过特征域上的访问控制结构来加密，用户能够对某个密文解密当且仅当他的特征集满足该密文中的访问结构。

当前绝大多数CP-ABE方案中，密文长度和加解密所需的计算量都随着访问结构中的特征个数呈线性增长，这导致密文长度过长，加解密速度很慢。而其余一些密文长度固定的CP-ABE方案中，对访问控制结构有很强的限制，比如单调性，只能实现与门结构，只能实现某种特殊的访问结构等等，这使得加密者不能灵活指定访问结构，因此这类方案不具有一般性。

本文中，我们构造了一个新的CP-ABE方案，其访问结构可以是任意的布尔函数，而密文长度和加解密所需计算量只随着布尔函数中析取范式的或门个数呈线性增长。基于熟知的判定性n-BDHE假设和碰撞稳固的哈希函数的存在性，可以在标准模型下证明它是CPA安全的。我们还给出了该方案的C程序实现，简单模拟了该方案的运行过程。

关键词：特征加密；布尔函数；密文规则；判定性n-BDHE假设

Abstract

Attribute-based encryption provides good solutions to the problem of anonymous access control by specifying access polices among private keys or ciphertexts over encrypted data. In ciphertext-policy attribute-based encryption(CP-ABE),each user is associated with a set of attributes,and data is encrypted with access structures on attributes. A user is able to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure.

Now in the most CP-ABE schemes, the encryption and decryption operations need large ciphertext and computation costs, which linearly depends on the number of attributes involved in the access policy.

Other CP-ABE schemes has a strong restriction on access control structure, while they have a fixed ciphertext size. For example, some schemes can only build for the monotone access control structure or the AND gate access policy and so on.This makes the scheme inflexible for use, so this schemes can not be impled in general way.

In this paper,we present a new CP-ABE scheme. Ciphertext size and comutation costs in the encryption and decryption operations only linearly depend on the number of OR gate in disjunctive normal form of Boolean functions. And our scheme can be impled in any Boolean function access control. The security of our scheme is proven to be CPA-secure in standard model under the decision n-BDHE assumption and the existence of collision-resistant hash functions. We also provide the C program at the end of this paper,as a simple simulation of the operation process of the scheme.

Key words: Attribute-based encryption; Boolean function; ciphertext-policy; decision n-BDHE assumption

目 录

Contents

第 一 章　引言

1.1　ABE的提出

信息安全是信息社会所关注的重要问题之一，而密码学是信息安全的核心技术。1949年，信息论创始人Shannon发表了《Communication Theory of Secrecy Systems》，使对密码的研究从一门艺术变为一门科学，标志着密码学这门新学科的诞生；1976年，Diffie和Hellman发表了《New Directions in Cryptography》，提出了公钥密码的思想，标志着现代密码学的开端。

与传统密码体制相比，公钥密码体制的加密密钥与解密密钥不同，虽然加解密速度较慢，但是较好地解决了传统密码体制中密钥分发和管理的难题，并能构造有效的数字签名方案，因此能够很好地为网络信息提供机密性、数据完整性、认证性和不可否认性等安全服务。

公钥密码体制是建立在单向陷门函数（One-way Trapdoor Function）上的，其安全性都是基于某种数学难题。1978年，Rivest、 Shamir和Adleman提出了RSA公钥密码体制，其安全性基于整数因子分解的数学难题，RSA是第一个实用的公钥密码体制，也是到目前为止应用最广泛的公钥密码体制。1985年，ElGamal提出了一种基于离散对数问题的公钥密码体制，称为ElGamal密码体制，后来的Schnor签名体制和数字签名标准DSA都是它的变形。1985年，Koblitz和Miller分别独立地提出了基于椭圆曲线离散对数问题的椭圆曲线密码体制，其短密钥高强度的特点使得它一直是密码学的研究热点之一。

在传统的公钥密码学中，公钥是与身份无关的随机字符串，存在如何认证公钥的真实性的问题。公钥基础设施（Public Key Infrastruction，PKI）通过使用可信第三方——签证中心（Certification Authority，CA）颁发公钥证书的形式来绑定公钥和身份信

息。不过，PKI证书管理复杂，需要建造复杂的CA，证书发布、吊销、验证和保存需要占用较多资源，这就限制了PKI在实时和低宽带的环境中应用。

为了简化公钥证书的管理，在1984年，Shamir革命性地引入了基于身份密码学（Identity-Based Cryptography，IBC）。在IBC中，公钥是代表用户身份的任意字符串，比如用户的名字、E-mail地址、手机号码等；存在一个可信任的机构——私钥生成器（Private Key Generator，PKG），根据用户的身份生成相应的私钥：首先运行Setup算法，生成系统的全局参数（或者称为主公钥）和主密钥；然后运行 Extract算法，输入主密钥和一个任意的身份$ID \in \{0,1\}^*$，输出相应的私钥。由于公钥直接从身份信息中提取，则证书和公钥目录是不必要的，因此简化了公钥的管理，并由此带来了不需要密钥信道的非交互式通信以及不需要证书校验，节约了计算和通信成本。

当某人想要分享一些敏感数据时，他可以建立一个访问控制规则，指定哪些人可以获得这些数据。传统的做法是，用一个可信任的服务器来存储这些数据，但这种方法有个缺点，这些数据是以明文形式存储在服务器中，一旦该服务器遭到黑客入侵，数据的安全性将不复存在。鉴于此，数据应该以密文的形式存储，这样的话，即使服务器遭到入侵，数据仍然是安全的。数据的提供者可以用接收者的公钥来对数据加密，于是，只有这些接收者可以利用他们的私钥对密文解密。然而，在很多应用中，我们想要将一些数据分享给某些人，而这些人我们事先并不知道他们是谁。在这种情形下，数据的提供者通常指定接收者应该具有的特征，比如他们的性别，年龄，工作，工作经验等，而不是具体指定是哪些人。访问控制规则指定了具有哪些特征的人可以对该数据进行访问。比如访问控制规则可能是“年龄大于等于m且工作年限大于等于n”，“具有某个职位或工作年限大于等于n”等等。因此，传统的基于身份的加密方案（IBE）并不能有效解决该问题，我们需要构造基于特征的加密方案（ABE）。

2005年，Sahai和Waters[1]对上述问题提出了一种解决方法，他们称之为基于特征的加密方案（ABE）。在ABE 系统中，数据加密方可以对数据指定一个访问结构，该访问结构可以被看作是特征域上的布尔公式。系统中的每个用户都从可信中心那里得

到一个私钥，这个私钥与他们的特征集相对应。用户可以用他的私钥解密某个密文当且仅当他的特征集满足密文中的访问结构。ABE系统应具有的一个重要的性质是抵抗共谋攻击：如果每个用户都不能解密某个密文，那么他们联合起来应该也不能解密该密文。

随后，Goyal，Pandey，Sahai和Waters[2]定义了两种形式的ABE：密钥规则的ABE（KP-ABE），特点是密文与特征集相联系，私钥与访问结构相联系；密文规则的ABE（CP-ABE），特点是私钥与特征集相联系，密文与访问结构相联系。[2] 给出了一个KP-ABE方案。 [3]给出了第一个 CP-ABE方案。随后，具有非单调访问结构的ABE方案在[4,5]中做了研究。

在提出特征加密的概念后，许多的ABE方案 [3–11]被构造了出来。在绝大多数的ABE方案中，密文的长度和加解密所需的计算量都（至少）随着访问结构中特征的个数呈线性增长，这阻碍了ABE在现实中的应用。如果考虑具有大量特征的访问结构，那么通信的带宽和加解密所需的计算量都将成为实际应用中的瓶颈。

选择明文安全（CPA-安全）和选择密文安全（CCA-安全）是公钥加密体制安全性中的重要概念 [12–17]。在公钥加密体制中，加密密钥是公开的，任何人都可以用它来对数据加密，因而敌手可以对方案进行选择明文攻击。这就使得CPA-安全成为了公钥加密体制安全性中的最低要求。CCA-安全是比CPA-安全更高的一个安全等级，它要求加密方案能够抵抗敌手在选择密文下所做的攻击。然而，利用现有的技术，可以很容易地将一个CPA-安全的密码方案转化为一个CCA-安全的密码方案，并且转化后方案的密文长度和加解密所需计算量并无本质上的增加。本文中，我们将致力于构造一个CPA-安全的特征加密方案，而省略了CPA-安全向CCA-安全的转化。需要指出的是，这个转化的思想是将签名应用到加密中，消息在加密时也做了签名，并将生成的签名嵌入密文中。解密时运行签名验证算法来验证密文的合法性，只有合法的密文才能够被解密。考虑到CCA-安全模型，这其实是限制了敌手做明文查询，使得敌手在CCA-安全模型中的能力在本质上与CPA-安全模型中的能力相同。从而将方案的安全

性从CPA-安全提升到CCA-安全。

1.2　本文主要工作

本文中，我们提出了一个CPA-安全的CP-ABE方案，其访问结构可以是任意的布尔函数，其密文长度和加解密所需计算量都只随布尔函数中或门个数呈线性增长。与之前的CP-ABE方案相比，我们的CP-ABE方案在加解密性能上要好一些，在访问结构上实现了最大灵活性，并且可以在标准模型下基于一个熟知的假设证明其安全性。

在所构造的CP-ABE方案中，公钥中的每个元素和主密钥中的每个元素都对应于一个特征值。私钥生成器在为用户生成私钥时使用了一个随机选取的群元素，这就抵抗了共谋攻击。在私钥生成阶段，主密钥中的每个元素产生私钥中的一个元素，其值由用户在该特征上的取值决定，加密者在加密时将访问结构中每个合取项对应于特征的公钥中的元素聚合起来，这样对应于每个合取项就得到一个群元素，再将这些群元素隐藏在有限域上的某个多项式中。将多项式的系数以指数的形式放到密文中。在解密时，用户将其满足的合取项对应于特征的私钥中的元素聚合起来，得到一个群元素，该群元素满足构造密文时的那个多项式，于是可以从密文中提取出明文。使用这种技术，可以使密文的长度只与访问结构中或门的个数有关系，而与与门的个数无关。对于不同的用户，其私钥元素不能聚合在一起来解密，因此抵抗了共谋攻击。

1.3　相关的工作

第一个密文长度固定的CP-ABE方案由[18]提出。它只能实现(n,n)-门限访问结构，只有具有n个特定特征的人才能解密密文。另一个密文长度固定的CP-ABE方案由[19]提出，它适用于(t,n)-门限的情形，至少拥有t个特定特征的人能够解密密文，其中门限值t由加密者设定。其加密时需要进行$n+t+1$个指数运算，解密时需要进行$O(t^2)$个指数运算。但是这个方案具有单调的访问结构，并且其安全性基于一个扩展的假设（aMSE-DDH）。最近，[20]利用一个新的高效的基于身份的撤销机制，构造了第一个密

文长度固定的，具有灵活非单调访问结构的KP-ABE方案。这个KP-ABE方案具有平方规模的私钥长度，加解密所需的指数运算量与相关的特征数量成正比。

[21]提出了一个密文长度固定的CP-ABE方案，但其访问结构只能是与门结构。本文所提出的方案在处理访问结构中的合取项时应用了[21]中的聚合技术。

先前提出的大多数ABE方案都在选择模型下证明其安全性，Lewko等人[9]采用[22]中的对偶加密技术实现了完全安全的ABE方案。Okamoto 和Takashima[8]给出了一个基于常规假设下完全安全的ABE方案。 [23]中提出的方案也是完全安全的。

第 二 章　预备知识

2.1　布尔函数的范式

本文提出的ABE方案中的访问结构可以是任意的布尔函数。由于任意布尔函数都有其等值的析取范式形式，因此我们在方案的构造中直接使用该布尔函数的析取范式。下面简要介绍有关命题公式范式的知识。

范式是公式的一种标准形式。从等值的意义上讲，一个真值函数，有许多不同形式的命题公式，例如

$$P \leftrightarrow Q = (P \to Q) \wedge (Q \to P) = (\neg P \vee Q) \wedge (P \vee \neg Q) = (P \wedge Q)(\neg P \vee \neg Q) = \cdots$$

但实际上，他们都是具有相同真值表的同一真值函数。

定义1：称一个命题公式G有合取范式，如果G满足：

（1）$G = A_1 \wedge A_2 \wedge \cdots \wedge A_n, (n \geq 1)$

（2）每个$A_i (i = 1, 2, \cdots, n)$都是$G$中所含某些命题变元及其否定的析取式。

这样的A_i称为简单析取式或子句。

定义2：称一个命题公式G有析取范式，如果G满足：

（1）$G = B_1 \vee B_2 \vee \cdots \vee B_m, (m \geq 1)$

（2）每个$B_i (i = 1, 2, \cdots, m)$都是$G$中所含某些命题变元及其否定的合取式。

这样的B_i称为简单合取式或短语。

像$(P \vee Q \vee R) \wedge (\neg Q \vee R)$就是一个合取范式，而$(P \wedge Q \wedge R) \vee (\neg Q \wedge R)$ 则是析取范式，特别一个命题变元P或它的否定$\neg P$既可以看做合取范式，也可以看做析取范式。

任一命题公式G的合取范式和析取范式总是存在的并且可以求得的。或者说，任一命题公式G都存在与之等值的合取范式和析取范式。只要首先把G等值归化到$\{\neg, \vee, \wedge\}$上，而后利用反演律将$\neg$移至命题变元前（即否定深入），再由重排律，结合